AFRL-IF-RS-TM-2006-2
Technical Memorandum
March 2006

AIR FORCE ENTERPRISE DEFENSE (AFED)

Northrop Grumman

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TM-2006-2 has been reviewed and is approved for publication.

APPROVED: /s/

BRIAN T. SPINK
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	MARCH 2006	Tech Memo Apr 03 – Aug 04

4. TITLE AND SUBTITLE
AIR FORCE ENTERPRISE DEFENSE (AFED)

5. FUNDING NUMBERS
C - F30602-99-D-0001/0020
PE - 33140F
PR - 7820
TA - JM
WU - 20

6. AUTHOR(S)
Lou Scheiderich

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Northrop Grumman
7575 Colshire Drive
McLean Virginia 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/IFGA
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TM-2006-2

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Brian T. Spink/IFGA/(315) 330-7596/ Brian.Spink@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***
Provided technical Information Assurance (IA) support to the Air Force Research Laboratory (AFRL) Defensive Information Warfare (DIW) Branch in the design, development, integration, installation and demonstration of the Air Force Enterprise Defense (AFED) and Automated Intrusion Detection Environment (AIDE) systems.

14. SUBJECT TERMS
Sort Finder, Drilldown

15. NUMBER OF PAGES
15

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

TABLE OF CONTENTS

LIST OF FIGURES

1.0 What is AFED?

AFED is a security management system combining data from multiple types of sensors including IDS, vulnerability assessment, change management, correlators, etc.

1.1 Allows analyst to view data from a single console.

1.2 Aggregation capabilities significantly reduce data that must be viewed by analysts.

1.3 AFED components are configurable and flexible to allow them to be quickly modified to accept, aggregate and display information from new data sources.

2.0 Background:

2.1 Development – 2000 to 2004

2.2 Built on EPIC, AIDE, EPIC2 systems

2.3 Started as AC2ISRC funded program, then supported by In-House funding

Initiated to address Warfighter needs for better network security tools

2.4 Installations at ACC NOSC (2000), AFIWC (2002) and AFRL/RRS NOC 2002

2.5 Core system completed Jan 2004

3.0 Before AFED:

3.1 EPIC (Extensible Prototype for Intrusion Control)

- 1997-1998
- Designed to collect information from Multiple Data Sources
- Based upon G2 Expert System
- Demonstrated at EFX 98, JBC 98

4.0 AIDE (Automated Intrusion Detection System)

4.1 1998 to 2002

4.2 DISA ATD built on EPIC focused on Intrusion Detection and Hierarchical Reporting.

4.2.1 Deployed to 15+ DISA sites

5.0 EPIC (Extensible Prototype for Intrusion Command and Control)

– 1999 to 2000
– Enhanced version of EPIC
– New features included
  – additional database support
  – Policy enforcement capability
  – Host information
  – Network Management

6.0 AFED Database

6.1 Application – Oracle 9i Database

6.2 Types of Data Stored

- Host/Network based intrusion detection events (including syslog events)
  . OS
  . Location
. Services/service approval status
  . POC data
  . Vulnerability data
  . Mission data

- Signature References, Analyst defined Notes/COA's
- Signature Normalization data
- IP domain to Organization mappings and metadata

7.0 DATA Extraction Utility

7.1 Application – Java based client/server

7.2 Capabilities

- Robust communication of data from files/databases to another database
- Supports Oracle, MySQL, Postgres, and Access
- Extreme configurability (configuration file specifies parsing, filtering, connections, etc.)

- Bookmarking

. Tracks what data was read and transferred
. Prevents loss of data in the event of a shutdown or network failure
. Source quenching
. Throttling mechanism that buffers data at server side to prevent overrun of database

- Health status reporting
- Can be used independently of AFED database and FlexViewer

8.0 SQL Correlator

8.1 Application

- Java based application based on FlexViewer
- Writes results to database

8.2. Capabilities

- Generate new "Cyber Alerts" regarding conditions that can be determined from SQL queries and insert then into database.
- Extreme configurability
- Read/write to any database schema
- Supports Oracle, MySQL, Postgres, and Access
- Can be used independently of AFED database and Data Extraction Utility and FlexViewer

9.0 FlexViewer

9.1 Application

- Java Based Graphical User Interface
- Provides a spreadsheet view of data
- Graphical capability to be added

9.2 Capabilities:

- Displays Data from Oracle, MySQL, Postgres, and Access
- Drive third party apps using data from spreadsheet cells
- Fully configurable menus
- User definable/sharable
- Built-in scripting engine allowing extreme extensibility
- Can be used independently of AFED database and Data Extraction Utility

10.0 AIDE (Automated Intrusion Detection System)

10.1 1999 TO 2000

10.2 Enhanced version of EPIC

10.3 New features included:

10.1.1 Additional database support

10.1.2 Policy enforcement capability

10.1.3 Host information

10.1.4 Network Management

AFED Conceptual Architecture

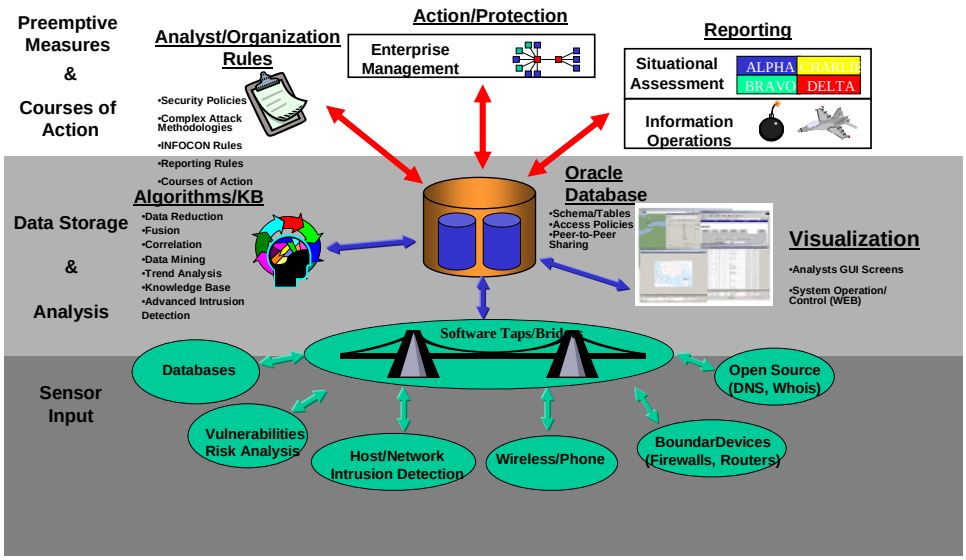

Figure 1: AFED Conceptual Architecture

AFED Components

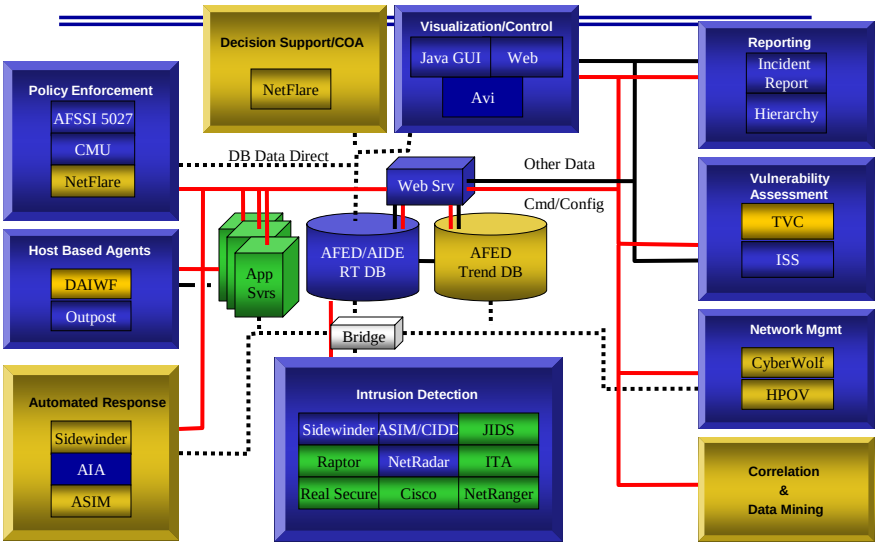

Figure 2: AFED Components

AFED FlexViewer

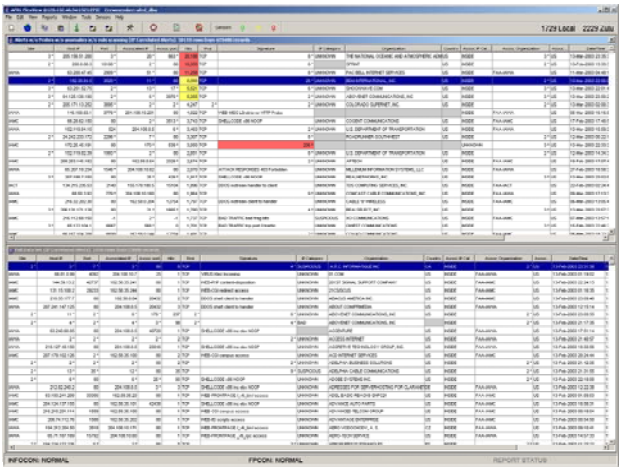

Figure 3: AFED FlexViewer

FlexViewer - Editor Window

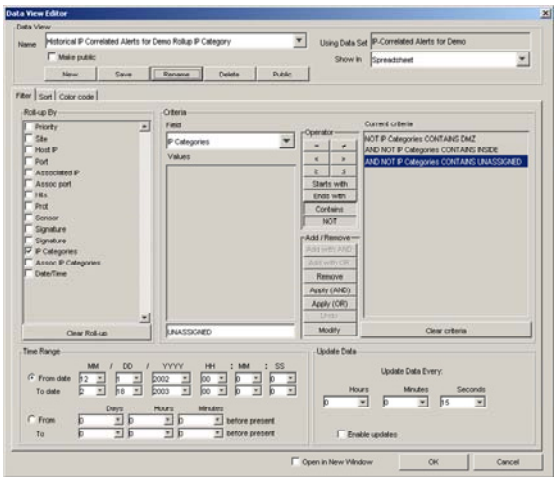

Figure 4: FlexViewer – Editor Window

FlexViewer - Sort Editor

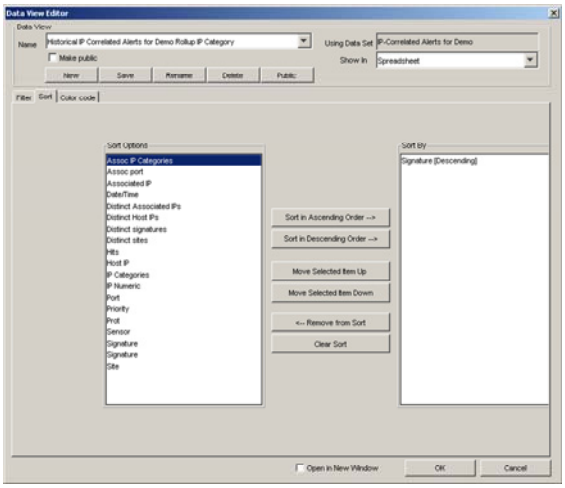

Figure 5: FlexViewer – Sort Finder

FlexViewer - Color Code Editor

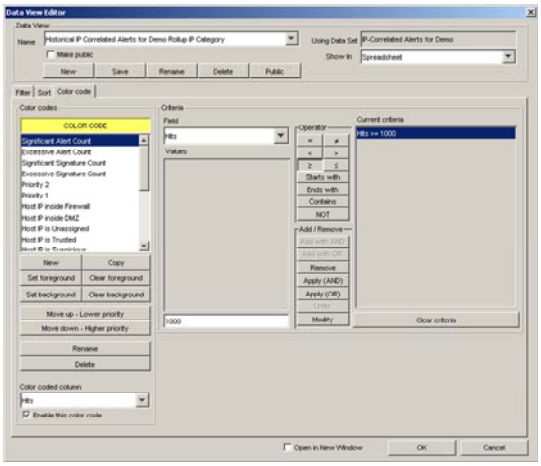

Figure 6: FlexView – Color Code Editor

FlexViewer - Color Codes Applied

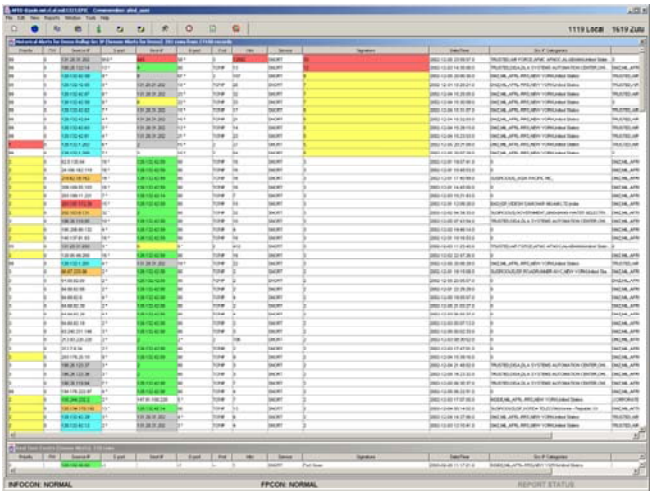

Figure 7: FlexViewer – Color Codes Applied

Host POC Drilldown

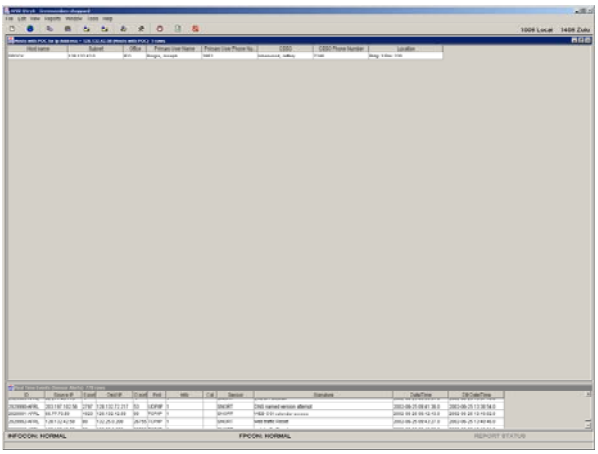

Figure 8: Hose POC - Drilldown

Host Services Drilldown

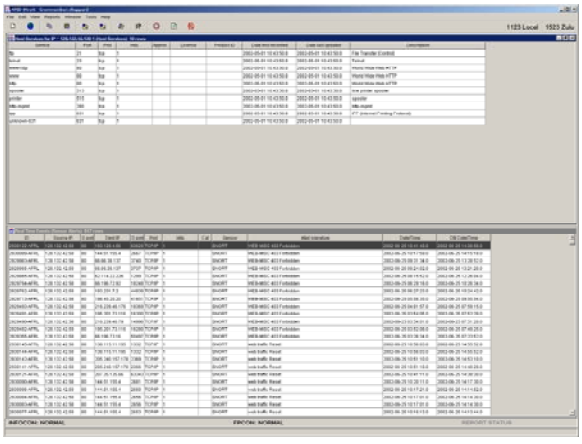

Figure 9: Hose Services - Drilldown

Data View

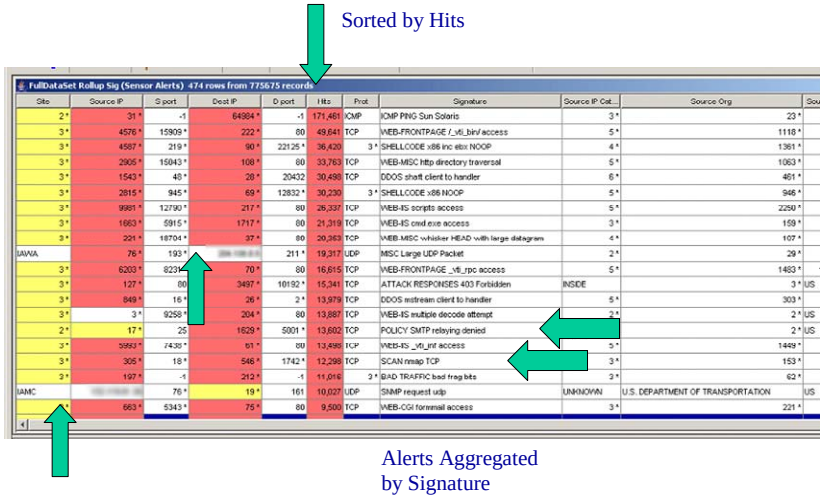

Figure 10: Data View

Data View - Tuning Applied

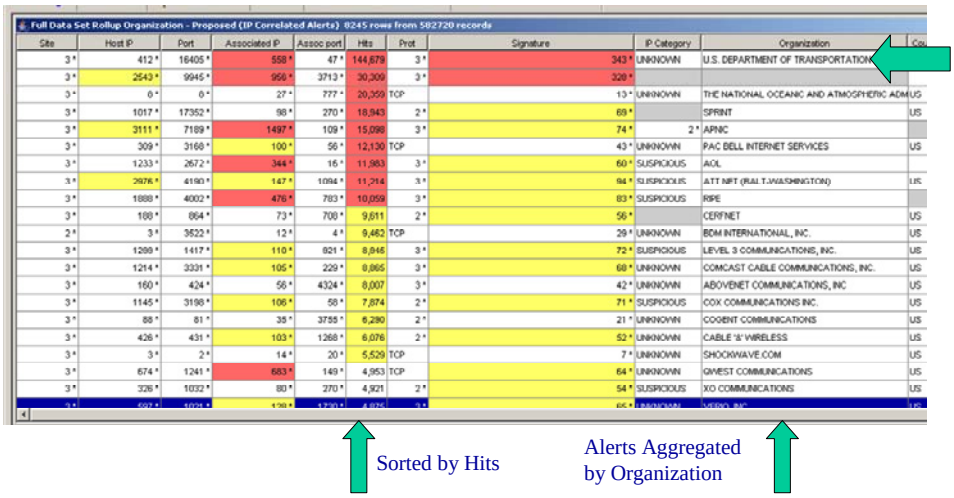

Figure 11: Data View – Tuning Applied

Data View - Organization Drilldown

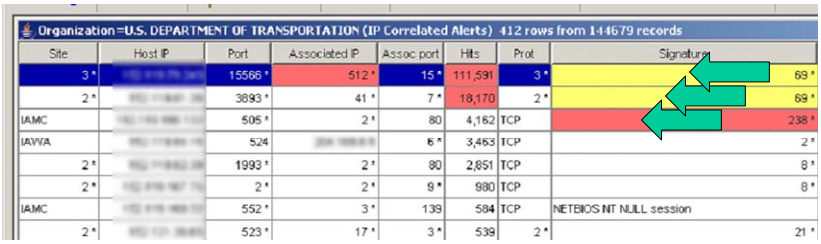

Figure12: Data View – Organization Drilldown